read,
基于激励的方案
激励值有统一的TTP发放
把中继节点的贡献时间（即消息持有的时间，该值在对加密链解密后由目的节点反馈给TTP）作为源节点支付给中继节点的信用值量从而提出EPSR方法，为了激励分叉节点在此基础上提出了EPCR方法，同时证明了所提出的方法能够应对转发路径的边插入、边删除攻击和内容修改攻击，且用来激励的信用值的具有上界。

A Secure Credit-Based Incentive Mechanism for Message Forwarding in Noncooperative DTNs

Honglong Chen, *Member, IEEE*, Wei Lou, *Member, IEEE*, Zhibo Wang, *Member, IEEE*, and
Qian Wang, *Member, IEEE*

***Abstract*—Delay-tolerant networks (DTNs) are an emergent communication paradigm characterized by intermittent connectivity. The nodes in DTNs can take advantage of their contact opportunities to forward messages. However, in noncooperative DTNs, the nodes may be selfish and reluctant to cooperate with each other in message forwarding. In such DTNs, stimulating cooperation among the nodes will be indispensable. Recently, many incentive mechanisms have been proposed to motivate nodes to cooperate in message forwarding. However, most of them cannot guarantee systematic security. To resolve the drawback of the previous incentive mechanisms, we first propose a credit-based rewarding scheme called the earliest path singular rewarding (EPSR) scheme to motivate the nodes to truthfully forward the messages during every contact opportunity. Then, we propose another credit-based rewarding scheme called the earliest path cumulative rewarding (EPCR) scheme by further considering that a node may get more contact information on others. We prove that both the EPSR and EPCR schemes are incentive compatible, and the payment for each delivered message is upper bounded. Furthermore, the proposed schemes can prevent selfish nodes having malicious behaviors. We have conducted real-trace-based simulations to illustrate the effectiveness of the proposed EPSR and EPCR schemes.**

***Index Terms*—Cooperation, noncooperative delay-tolerant networks (DTNs), rewarding schemes, secure.**

I. Introduction

As an emergent communication paradigm, delay-tolerant networks (DTNs) [1]–[3] are competent for many applications, such as vehicular networks [4]–[6], mobile social networks [7], [8], and pocket switched networks [9]. However, DTNs often experience intermittent connectivity due to the high mobility or sparse deployment of the nodes, in which there are generally no stable end-to-end delivery paths. Therefore, the traditional routing protocols are not applicable for the intermittently connected DTNs. Epidemic routing [10] is a simple but competitive DTN routing protocol, in which each node will fully make use of every contact opportunity to replicate the messages to its encounter. Although epidemic routing may introduce a high overhead, it can be easily implemented in applications and achieve satisfying performance [11], [12].

In noncooperative DTNs [29], the nodes may be managed by some rational individuals [13], such as human beings or other autonomous parties. Such nodes may be selfish [6], [11], [12], [14], [15], i.e., they only aim to maximize their individual utilities and will not be willing to cooperate with others to truthfully forward the messages if they can make no profit from message forwarding, or they may even conduct some malicious behaviors to get extra profit from message forwarding. Due to the distributed characteristic of DTNs, it is difficult to detect and prohibit the selfish behaviors conducted by the individual nodes. Therefore, it is necessary to have an efficient incentive mechanism for the noncooperative DTNs to stimulate cooperation among the selfish nodes in message forwarding.

Generally, the incentive mechanisms can be classified into three categories [15]: reputation-based, credit-based, and tit-for-tat-based (TFT-based) schemes. The reputation-based schemes require each node to monitor the traffic information of all its neighbors and keep track of their reputations, which should be propagated to all other nodes efficiently and effectively. The TFT-based schemes require each node to detect the misbehavior of its neighbors. It would be difficult to achieve direct traffic monitoring or misbehavior detection in intermittently connected DTNs. On the other hand, credit-based schemes use virtual credits to motivate selfish nodes to participate in the message forwarding, and the credits they earned from forwarding other nodes' messages can be used to pay for the delivery of their own messages. Furthermore, the rewarding process can be conducted by a central manager, the communication between which and the nodes is delay tolerant. The given characteristics of credit-based schemes make them suitable for DTNs. Therefore, we will adopt the credit-based incentive scheme in this paper to stimulate nodes' cooperation.

Manuscript received April 6, 2015; revised June 29, 2015; accepted August 18, 2015. Date of publication September 7, 2015; date of current version August 11, 2016. This paper was presented in part at the IEEE International Conference on Computer Communications and Networks. This work was supported in part by the National Natural Science Foundation of China under Grant 61309023, Grant 61272463, Grant 61373167, and Grant 61502352; by the Shandong Provincial Natural Science Foundation, China, under Grant ZR2013FQ032; by the Shandong Provincial Key Program of Research and Development under Grant 2015GGX101045; by the Hong Kong General Research Fund under Grant PolyU-524308 and Grant PolyU-521312; by The Hong Kong Polytechnic University under Grant A-PJ16, Grant A-PL84, Grant 1-VZ5N, and Grant 4-BCB6; by the Natural Science Foundation of Hubei Province under Grant 2013CFB297 and Grant 2015CFB203; by the Natural Science Foundation of Jiangsu Province under Grant BK20150383; and by the Wuhan Science and Technology Bureau under Grant 2015010101010020. The review of this paper was coordinated by Prof. Y. Cheng.

H. Chen is with the College of Information and Control Engineering, China University of Petroleum, Qingdao 266580, China, and also with the Department of Computing, Hong Kong Polytechnic University, Kowloon, Hong Kong (e-mail: chenhl@upc.edu.cn).

W. Lou is with the Department of Computing, Hong Kong Polytechnic University, Kowloon, Hong Kong, and also with Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen 518057, China.

Z. Wang and Q. Wang are with the School of Computer, Wuhan University, Wuhan 430072, China.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2015.2477164

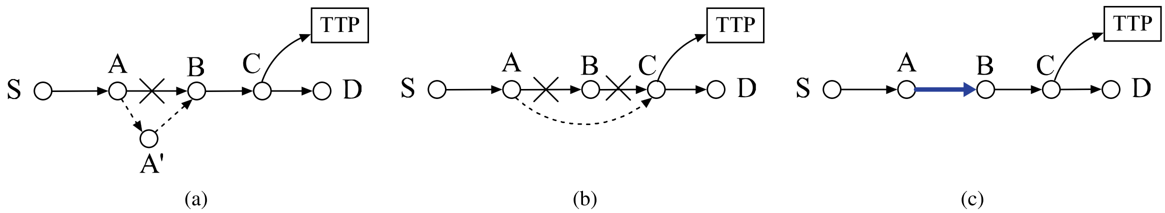

Fig. 1. Edge insertion attack, (b) edge removal attack, and (c) content modification attack.

MobiCent [12] is a recently proposed credit-based incentive scheme for mobile ad hoc network routing, in which the payment mechanism is based on the hop count of the delivery path. MobiCent is proved to be incentive compatible (i.e., the truthful cooperation is the dominant strategy of each of the nodes), and it can guarantee that the payment for each delivered message is upper bounded, which is a typical drawback of the Vickrey–Clarke–Groves (VCG)-based incentive schemes [14], [16]. It is also a defense mechanism against the security threat of an *edge insertion attack* (a kind of sybil attack), in which a node can forge a virtual edge into a path to get extra reward, and this kind of attack cannot be solved in SMART [17]. However, MobiCent suffers the *edge removal attack*, in which two nodes can collude with each other to get extra payoff by removing the record of relaying behavior of one of them. For example, as shown in Fig. 2, node S generates a message with destination node D. The message is delivered to the destination along three paths, among which path $P = S \rightarrow A \rightarrow B \rightarrow C \rightarrow D$ has the least hop count; then, each node in path P will get a reward of $(2+\epsilon)^{N-n}$ cents according to MobiCent, where N is the maximum path length, n is the hop count of path P, and ϵ is a small positive natural number. Suppose $N = 5$; then, $n = 3$ (the length of the path in MobiCent is the number of relay nodes on the path). Hence, each of the nodes A, B, and C will get a reward of $(2+\epsilon)^{N-n} = (2+\epsilon)^2$ cents. However, according to the rewarding mechanism, each node in the shortest path can get more reward if the number of hops is smaller, and then, they will have the motivation to collude with each other to deliberately shorten the path to get more reward. For instance, nodes A and B can collude with each other to act as a single node, and then, the hop count of path P will be 2, and they will get a total reward of $(2+\epsilon)^3$ cents. Finally, each of nodes A and B will get $(2+\epsilon)^3/2 = (1+\epsilon/2)(2+\epsilon)^2$ cents, which is larger than the original value. Therefore, it is necessary to design a secure incentive mechanism to simultaneously resolve the aforementioned drawbacks of the previous credit-based incentive schemes.

这种欺骗方案可以获得更多的收益

In this paper, we consider the following three typical malicious behaviors of the selfish nodes, which can seriously disturb the credit-based incentive schemes.

1) *Edge insertion attack (or sybil attack)*: A selfish node may attempt to forge a virtual edge (or a sybil node) into a path to get extra reward from the system. As shown in Fig. 1(a), node A may forge a sybil node A' between node B and itself, and then, the reward to node A' will be essentially obtained by node A.
2) *Edge removal attack*: A selfish node may attempt to remove or hide the forwarding behaviors of other nodes in a path to get more reward, which should be originally paid to the removed nodes. As shown in Fig. 1(b), node C may remove the edges $\overrightarrow{AB}$ and $\overrightarrow{BC}$ and cheat the system that the message it has received is directly from node A, but not node B; then, node B will get no reward, which benefits node C.
3) *Content modification attack*: A selfish node, or several colluding nodes, may attempt to modify the content of the report message, which contains the path information, such as the transmitting time and receiving time. As shown in Fig. 1(c), when node A forwards a message to node B, it may determine to modify the content of the message to get benefit. Since the reward may be calculated based on the report message, each node will have the motivation to launch a content modification attack to get more reward.

The design goals of our proposed incentive mechanisms in this paper are threefold: 1) incentive compatibility: to make truthful forwarding be the dominant strategy for all the nodes; 2) budget control: to guarantee that the payment for each delivered message is upper bounded; and 3) security enhancement: to defend against the above typical attacks. By considering the design goals, we first propose a credit-based rewarding scheme called the earliest path singular rewarding (EPSR) scheme to motivate the nodes to truthfully forward the messages during every contact opportunity. By further considering that a node may get more contact information on others and misbehave accordingly to take advantage of that, we then propose another credit-based rewarding scheme called the earliest path cumulative rewarding (EPCR) scheme. The main idea of the proposed rewarding schemes is to reward each node in the earliest delivery path according to its *contribution time*, which is the period of time that the node holds the message.

The main contributions of this paper are summarized as follows.

- We propose two rewarding schemes, namely, EPSR and EPCR, to stimulate cooperation among the nodes in message forwarding for noncooperative DTNs. The proposed schemes are incentive compatible when properly setting the initial financial deposit of each node.
- We prove that the payment for each delivered message in the two proposed rewarding schemes is upper bounded. Thus, the rewarding schemes can work even when the nodes have a finite budget.
- The proposed rewarding schemes can prohibit the typical malicious behaviors of the selfish nodes.
- We conduct the simulations based on the real trace to analyze the effects of the selfish nodes on the routing performance and illustrate the effectiveness of our proposed rewarding schemes.

The rest of this paper is organized as follows. In Section II, we give an overview of the epidemic-based routing protocols and the related incentive schemes. Section III proposes the system model. In Section IV, we propose the earliest path singular rewarding scheme. In Section V, we propose the EPCR scheme. The performance evaluation is briefly presented in Section VI. Section VII concludes this paper.

II. Related Work

Here, we will first review the epidemic-based routing protocols in DTNs. Then, we will discuss the existing three types of incentive schemes: reputation-based, credit-based, and TFT-based.

A. *Epidemic-Based Routing Protocols*

Routing in DTNs is a challenging issue since the nodes are intermittently connected and a lot of uncertain factors (such as the uncertain mobility of nodes) exist during the procedure. Thus, epidemic-based routing protocols [10], [18]–[20], in which each node will fully make use of every contact opportunity to replicate the messages to its encounter, will be a competitive choice in DTNs. Vahdat and Becker proposed the first epidemic-based routing protocol [10], in which each message is replicated and flooded to all the nodes in the network. However, it involves a huge overhead since the number of replicas of each message rapidly increases. In Prophet [18], a node will replicate and forward a message to its encounter only if its encounter has higher likelihood of meeting the destination, which can reduce the overhead. In MaxProp [19], due to the limitation of buffer space, each node schedules both the packets to be transmitted to other nodes and the packets to be dropped. In delegation forwarding [20], the message is replicated and delivered by a node to its encounter only if its encounter has a better quality metric, which can reduce the cost to $O(\sqrt{n})$, compared with the cost $O(n)$ of the routing protocol in [10], where n is the number of nodes in the network.

B. *Incentive Schemes*

In noncooperative DTNs, the epidemic-based routing protocols cannot work without appropriate incentive schemes. To solve this problem, many incentive schemes [12], [14], [21]–[23] have been proposed. The incentive schemes for the message forwarding can be generally classified into reputation-based schemes, credit-based schemes, and TFT-based schemes.

In the reputation-based incentive schemes, each node will monitor its encounters' traffic information and keep track of the reputation of all the other nodes. The reputation of a node will increase when it forwards a message, which is eventually delivered successfully. Based on the node's reputation, differential services will be provided. In [21], a secure and objective reputation-based incentive scheme called SORI is proposed to encourage the node to forward the message truthfully and discipline the node's selfish behaviors, in which the reputation of a node is quantified by objective measures, and the propagation of reputation is efficiently secured by a one-way-hash-chain-based authentication scheme. CONFIDANT [24] is proposed to make the misbehavior unattractive, which is based on selective altruism and utilitarianism. It aims at detecting and isolating the misbehaving nodes to make it unattractive for each node to decline the cooperation. Uddin *et al.* proposed a rewarding scheme called RELICS [22], which provides incentive to nodes in a physically realizable way in that the rewards are reflected into network operations. The ranking (reputation) of nodes depending on their transit behaviors is employed, and those ranks are translated into the message priority in the forwarding.

The credit-based incentive schemes motivate each node to help in forwarding the messages of others to earn virtual credits, which the node can use when it wants to deliver its own generated messages. A Trusted Third Party (TTP) is a necessity in the credit-based incentive schemes to manage the rewarding procedure. In [25], an incentive data collaboration scheme is proposed to encourage user participation of selfish nodes in DTNs. Zhong *et al.* [14] proposed an incentive scheme based on the VCG mechanism to select the best available single path for the message forwarding. Another VCG-based incentive scheme proposed in [16] uses a principal-agent model to motivate message forwarding in multihop wireless ad hoc networks with hidden information and actions. However, the VCG-based incentive schemes are known to suffer from the sybil attack, and they cannot guarantee that the payment for each delivered message is finite. In SMART [17], the layer coin is employed in the proposed incentive scheme, which can be a defense against several attacks but not the sybil attack. The MobiCent proposed in [12] is a credit-based incentive system that motivates epidemic routing in DTNs, which can be a defense against the edge insertion attack and the edge hiding attack. However, it cannot solve the scenario when two nodes collude together to reduce the hop count of a path to cheat the system for the extra reward.

In TFT-based incentive schemes, a node will fully cooperate with its neighbor if no misbehavior is detected, and it will gradually lower service to a neighbor whose cheating is detected. In [13], an incentive-aware routing protocol in DTNs is proposed to adaptively optimize individual performance subject to TFT without significant degradation of system performance. MobiTrade [26] is another TFT-based scheme, which proposes a utility-driven trading system to optimize the content-sharing strategy in DTNs and derives an optimal policy to split the buffer of a node in zones allocated to each channel. ConSub [15] proposes a content exchange protocol between two interacting nodes and encourage them to play as businessmen and carry contents to satisfy each other's interest.

In this paper, we choose the credit-based incentive scheme as the basis to design the rewarding schemes for the message forwarding in the noncooperative DTNs to overcome the drawbacks of the aforementioned incentive schemes.

III. System Model

In this paper, we consider a DTN formed by n mobile nodes. When two nodes encounter each other, they will exchange the messages in their buffers according to the priority of each message. Various DTN routing protocols have different message priorities. In the epidemic routing protocol, all messages have

借助TTP进行身份验证和奖励发放，
VB虚拟银行
可能是low-bandwidth long-range link

TABLE I
TERMINOLOGY

Notation	Definition
n	Number of nodes in the network
e	A delivery edge
t(e)	Contact time of edge e
P	A delivery path
t(P)	Delivery time of path P
TTP	Trusted third party
VB	Virtual bank
TTL	Time-to-live of each newly generated message
$Ct(v_i, P)$	Contribution time of node v_i in path P
PK_i	Public key of node v_i
RK_i	Private key of node v_i
$Rd(v_i, m_k)$	Reward to node v_i for the delivery of message m_k
t_i^t	Transmitting time of node v_i
t_i^r	Receiving time of node v_i
$Pay(S, m_k)$	Payment of source node S for the delivery of message m_k
$Fn(P_i, P_j)$	Furcation node of two paths P_i and P_j
T	Time period to transmit a unified-size message
$\mathbb{P}^k$	Set of all delivery paths of message m_k

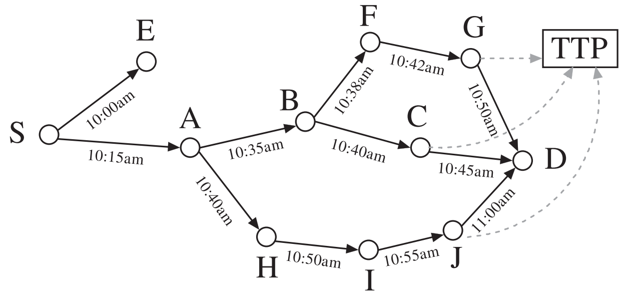

Fig. 2. Example of the rewarding process for the message forwarding in a DTN. A message is generated by node S at 9:55 A.M. The solid-line arrows and the dashed-line arrows indicate the short-range high-bandwidth links and the long-range low-bandwidth links, respectively. The timestamp under each solid-line arrow indicates the transmitting time of the message.

the same priority, and each node will make use of every contact opportunity to replicate its held messages to its encounter.

To facilitate the description of the proposed rewarding schemes, we first give the following definitions: An *edge* $e = (\{v_i, v_j\}, t(e))$ is used to present an opportunistic link between two encountering nodes, where $\{v_i, v_j\}$ are the two nodes, and $t(e)$ is the contact time of e. It is denoted that $v_i \in e$ and $v_j \in e$ for the edge $e = (\{v_i, v_j\}, t(e))$. A *delivery path* $P = \{e_1, e_2, \ldots, e_m\}$ is used to present a message forwarding path from a source node to a destination node, where $e_1, e_2, \ldots, e_m$ are a sequence of edges listed in a nondecreasing order of the contact time. Two adjacent edges share a common node. The *delivery time* of a message on a path, i.e., $t(P)$, is defined as the contact time of the last edge on the path, i.e., $t(P) = \max_{e_i \in P} \ t(e_i)$. A node $v_i \in P$ if there exists $e_j \in P$ such that $v_i \in e_j$. The corresponding notations in this paper are defined in Table I.

Fig. 2 shows a sample DTN. $e = (\{A, B\}, 10{:}35$ A.M.$)$ denotes a link between nodes A and B at 10:35 A.M. The path $S \to A \to B \to C \to D$ is denoted as $P = \{(\{S, A\}, 10{:}15$ A.M.$)$, $(\{A, B\}, 10{:}35$ A.M.$)$, $(\{B, C\}, 10{:}40$ A.M.$)$, $(\{C, D\}, 10{:}45$ A.M.$)\}$. The delivery time of a message from nodes S to D on this path is at 10:45 A.M. nodes S, A, B, C, D are all $\in P$.

To motivate message forwarding in the noncooperative DTNs, a TTP is required to manage the rewarding process, i.e., to store the key information of the nodes and provide verification and payment services for the nodes that participate in the message forwarding. The TTP can be a running server that acts as a central controller. Each node can use the short-range high-bandwidth links to exchange messages with its encounters; it can also use the long-range low-bandwidth links to communicate with the TTP for the verification and payment during the rewarding process. A virtual bank (VB) is also needed, which is managed by the TTP. The VB will take charge of the credits of each node. For example, it should provide each node an account for saving its virtual credits earned from the message forwarding operations.

消息成功投递以后，最后一跳向TTP发送message，以发放激励

In the incentive mechanism, each relay node can add some path information, including its ID, receiver ID, receiving time, and transmitting time, onto the message when forwarding the message. After the message reaches the destination, the last intermediate node will extract the path information from the message and submit it as a *report message* to the TTP. The TTP calculates the rewarding credits for each relay node based on the report message and charges the source node for the corresponding credits. As shown in Fig. 2, node S generates a message m_k for destination node D. m_k will be delivered to node D by nodes C, G, and J along three different paths, respectively. Nodes C, G, and J will also submit the report messages to the TTP. The TTP can then conduct the rewarding process to reward each node according to the specific rewarding scheme.

Since the size of the report message is much smaller compared with that of the data message, the overhead caused by the report message, which will be submitted to the TTP by the last transmitter, can be ignored.

【思考】：是否可以用签名机制，来避免使用中央控制器TTP？（网络规模的扩展性差＋额外的通信支出）--像区块链那样

IV. EARLIEST PATH SINGULAR REWARDING SCHEME

Here, we first introduce the concept of contribution time in message delivery, which will be used in our proposed incentive schemes. Then, we describe the EPSR scheme and provide its related analysis.

A. Contribution Time in Message Delivery

To motivate the nodes in the message forwarding, the credit-based incentive schemes will reward the nodes that contribute to the delivery of a message based on a certain contribution metric. In our scheme, we choose the *contribution time* as the metric to measure the contribution of a node on the delivery of a message. The contribution time of a node in a delivery path of message m_k starts from the moment this node receives m_k and ends at the moment it transmits m_k to the next node in the path. It is easy to see that the contribution time of the source node begins from the moment the message is generated and the destination node has no contribution time in the path. For an intermediate node v_i in a path P, its contribution time in P can be denoted as $Ct(v_i, P)$, which can be formulated as

$$Ct(v_i, P) = \max_{v_i \in e_j, e_j \in P} t(e_j) - \min_{v_i \in e_j, e_j \in P} t(e_j). \quad (1)$$

v1写入E1

table 详细记录了 贡献时间

For the sample DTN shown in Fig. 2, assume that node S generates a message for destination node D at 9:55 A.M. After the delivery of the message, the contribution time of nodes S, A, B, and C in the path $S \to A \to B \to C \to D$ is 20 min (10:15 A.M. – 9:55 A.M.), 20 min (10:35 A.M. – 10:15 A.M.), 5 min (10:40 A.M. – 10:35 A.M.), and 5 min (10:45 A.M. – 10:40 A.M.), respectively.

Suppose that a message is generated by a source node with a time-to-live TTL.[1] The message has been delivered along a path P to the destination, and the residual time of the message when it arrives at the destination is t_r. Then, we can easily get

$$\sum_{\forall v_i \in P} Ct(v_i, P) = \mathrm{TTL} - t_r. \qquad (2)$$

总的贡献时间，
也即 所有中继持有
消息的时间之和

Since the nodes in a path cannot easily modify the total contribution time without affecting other nodes' contribution time, we will take advantage of this property by using the contribution time of each node as the rewarding basis.

B. EPSR Scheme

As we motivate the nodes to forward messages during every contact, the message generated by the source node will be delivered to the destination via different paths. The main idea of the EPSR scheme is to only reward the nodes in the earliest delivery path of the message. The reward to each node is calculated based on its contribution time in the earliest delivery path of the message, and all the rewards for the successful delivery of the message are paid by the source node.

The EPSR scheme has four phases: system initialization, message generation, message forwarding, and rewarding and charging.

1) System Initialization: As the rewarding procedure will be conducted by the TTP after analyzing the submitted report messages, it is significant to protect the integrity of the report messages to prevent the contribution time from being modified (by the content modification attack). In this paper, we adopt the asymmetric cryptographic method [27] to encrypt the report messages. In the initialization phase, the system generates n pairs of public/private keys. The TTP holds the private keys and distributes the public keys to each of the nodes. Thus, the TTP acquires the information of the corresponding relationships between the private keys and nodes. We denote PK_i as the public key of node v_i and RK_i as the corresponding private key of v_i, which is obtained by the TTP. Note that $PK_i \neq PK_j$ when $i \neq j$. We also denote $\mathrm{Enc}(PK_i, m_k)$ as the encrypted message m_k using the public key PK_i and $\mathrm{Dec}(RK_i, m_k)$ as the decrypted message m_k using the private key RK_i. Obviously, $\mathrm{Dec}(RK_i, \mathrm{Enc}(PK_i, m_k)) = m_k$.

2) Message Generation: When the source node generates a message, which has to be delivered to the destination within the TTL, it will simultaneously create a contribution table and attach it onto the message. As shown in Fig. 3, assume node v_1 is the source node that generates a message to destination v_m, v_1 will create the contribution table including the header and elements. The header contains the information of the source node ID, the destination node ID, the TTL of the message, and the generated time of the message (denoted as t_g), which is filled by the source node. Each of the elements will be added by each of the intermediate nodes when the message is forwarded. Note that a source node with a balance less than a threshold cannot generate the message anymore since it may not be able to pay for the delivery of such message, and if a source node violates the given rule, it will be easily detected by the TTP.

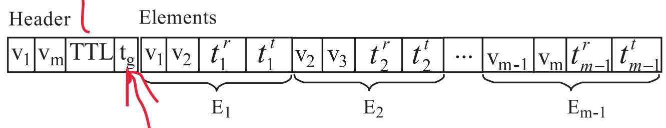

Fig. 3. Contribution table of the delivery path $v_1 \to v_2 \to \cdots \to v_m$ with source node v_1 and destination node v_m. The content in the elements is encrypted with the corresponding public keys.

若源节点支付不起payoff，则源
节点就不能再生成pkt

3) Message Forwarding: When an intermediate node, take node v_i for example, forwards the message to its encounter v_{i+1}, it will add a new element E_i onto the contribution table of this message. E_i contains transmitter ID v_i, receiver ID v_{i+1}, the time v_i receives the message, and the time v_i transmits the message to v_{i+1}. To guarantee the integrity of the contribution table, v_i can encrypt the element using its public key PK_i, i.e., $E_i = \mathrm{Enc}(PK_i, v_i \| v_{i+1} \| t_i^r \| t_i^t)$, where t_i^r denotes the time v_i receives the message, and t_i^t denotes the time v_i transmits the message. We assume that the drifted clock time among the nodes in the network is negligible. Note that it must satisfy $t_i^t > t_i^r$ and $t_i^t = t_{i+1}^r$ when $i < m - 1$. As shown in Fig. 3, when source node v_1 meets v_2, it will transmit the message to v_2, before which v_1 adds an element $E_1 = \mathrm{Enc}(PK_1, v_1 \| v_2 \| t_1^r \| t_1^t)$ onto the contribution table, where t_1^r is the time v_1 generates the message, i.e., $t_1^r = t_g$, and t_1^t is the time v_1 transmits the message to v_2, i.e., $t_1^t = t_2^r$. To make sure this equation is satisfied, the transmitter can timestamp the transmitting time onto the message, after which the receiver can check whether this time is consistent with its current time clock (a certain deviation is allowed), and considers it as the receiving time.

4) Rewarding and Charging: When the last intermediate node, i.e., v_{m-1} in Fig. 3, delivers the message to the destination, it will add an element $E_{m-1} = \mathrm{Enc}(PK_{m-1}, v_{m-1} \| v_m \| t_{m-1}^r \| t_{m-1}^t)$ onto the contribution table and submit the whole contribution table as the report message to the TTP. After receiving the report message, the TTP will first decrypt it using the corresponding private keys. As shown in Fig. 3, the TTP can first obtain the source ID v_1 and the destination ID v_m from the header, which is not encrypted. Then, it can use the private key RK_1 corresponding to the source node v_1 to decrypt E_1 as $\mathrm{Dec}(RK_1, \mathrm{Enc}(PK_1, v_1 \| v_2 \| t_1^r \| t_1^t)) = v_1 \| v_2 \| t_1^r \| t_1^t$. As E_1 contains the ID of the next relay node v_2, the TTP knows the corresponding private key RK_2 of E_2, and it can use RK_2 to decrypt E_2. Similarly, the TTP can decrypt all the elements one by one in a chain-decryption way.

链式解密结构

To motivate the cooperation among the nodes in the message forwarding, the TTP will reward some credits to the nodes that contribute to the delivery of the message. We denote the set of all the delivery paths of message m_k as $\mathbb{P}^k$. In the EPSR scheme, only the nodes in the earliest delivery path P, i.e., the

[1] The TTL used in this paper is measured in the scale of time unit but not hop count.

似乎可以做出来一个。

开始时 分配少量的credit，让它们支付消息的投递。系统才能转得起来。

存在加入的费用，节点不会使用不同身份。

delivery path with the shortest latency, can get the reward for the delivery of m_k. P can be formulated as

最小延迟路径的定义

$$P = \arg\ \min\left\{t(P_i)|\forall P_i \in \mathbb{P}^k\right\} \tag{3}$$

where $t(P_i)$ is the delivery time of path P_i. Note that for each message, different delivery paths will have different delivery times; thus, the TTP can easily select the delivery path with the shortest latency according to (3). The reward to each node v_i in P is

奖励的值 设定为 贡献时间

$$Rd(v_i, m_k) = Ct(v_i, P) \tag{4}$$

where $Ct(v_i, P)$ is formulated in (1). The reward, which is denoted as $\text{Pay}(S, m_k)$, to be paid by the source node is

$$\text{Pay}(S, m_k) = \sum_{\forall v_i \in P} Rd(v_i, P). \tag{5}$$

As shown in Fig. 2, source node S generates a message m_k at 9:55 A.M. for destination D, and m_k is delivered along three paths to D. When the last intermediate nodes of the three paths, i.e., nodes C, G, and J, deliver m_k to D at 10:45 A.M., 10:50 A.M., and 11:00 A.M., respectively, each of them will submit the report message to the TTP, respectively. After decrypting the submitted report messages, the TTP can determine that the path $P = S \to A \to B \to C \to D$ is the earliest delivery path of m_k according to (3). As the contribution time of nodes A, B, and C is $Ct(A,P) = 20$ min, $Ct(B,P) = 5$ min, and $Ct(C,P) = 5$ min, according to (4), $Rd(A, m_k) = 20$, $Rd(B, m_k) = 5$, and $Rd(C, m_k) = 5$.[2] Thus, $\text{Pay}(S, m_k) = 30$.

【思考】payoff根据经济理论里的相对优势来决定？

【思考】如何处理wandering attack？在dest节点周围游走 以获取更多的时间权重

C. Analysis

Here, we will analyze the EPSR incentive compatibility, budget issue, and security.

1) Incentive Compatibility: A rewarding scheme is considered to be *incentive compatible* if truthful cooperation (i.e., truthfully forward the message during each contact) is adopted by all the nodes, despite their selfish nature. As shown in Fig. 2, when node A meets node B at 10:35 A.M., it forwards m_k to B, and finally, the earliest delivery path will be $P = S \to A \to B \to C \to D$ and $Rd(A, m_k) = 20$. However, if A does not forward m_k to B at 10:35 A.M., instead, it chooses to forward m_k to H at 10:40 A.M., then the earliest path will be $P = S \to A \to H \to I \to J \to D$ and $Rd(A, m_k) = Ct(A, P) =$ 10:40 A.M.—10:15 A.M. $= 25$. Thus, we need to examine whether the EPSR scheme is incentive compatible, i.e., if node A will truthfully forward m_k to node B at 10:35 A.M. or not.

The incentive compatibility of the EPSR scheme relies on the *risk aversion* nature of individuals. Risk aversion refers to the reluctance of an individual to accept a bargain with an uncertain payoff rather than another bargain with a more certain, but possibly lower, expected payoff. The individual with risk aversion is apt to choosing a strategy with a higher probability to get the payoff. In the noncooperative DTNs, whether a node is risk averse or not depends on its current financial status. A node with a limited deposit tends to behave in a risk-averse way since it has to maximize the probability to get the reward to increase its deposit, which will be used to pay for the delivery of its own generated message. In the initialization phase of the proposed EPSR scheme, the system will allot a small amount of credits to each node, which can only afford the delivery of several messages. We assume that fabricating an identity requires some cost such as the registration fee, which is more than the allotted credits; hence, each node has no incentive to use a different identity to benefit from the initially allotted credits. Thus, each node will act in a risk-averse way during the routing procedure.

激励相容 来源于 风险规避；
也即节点不愿意接受那些收益不确定的交易，相对于收益确定（可能是更低的平均收益）的交易而言，

用博弈方法证明 更合适？

Theorem 1: The EPSR scheme is incentive compatible.

Proof: As each node in the network will act in a risk-averse way, it will always take a strategy to maximize the probability of getting the reward. Assume that node v_i holds a message m_k, when it meets node v_j, it has two candidate strategies: forwarding m_k to v_j or not. If v_i forwards m_k to v_j, the probability that it is in the earliest delivery path of m_k will increase,[3] indicating that v_i will have a higher probability to get the reward. However, if v_i declines to forward m_k to v_j, the probability for v_i to be in the earliest path of m_k will decrease. As a risk-averse node, v_i will decide to truthfully forward m_k to v_j to maximize its probability of getting the reward. Thus, the EPSR scheme is incentive compatible. ■

2) Budget Issue: When each node has a finite budget, an important consideration for the reward system is to control the rewarding credits for each transaction to avoid budget deficit for any node. In the EPSR scheme, for each delivered message, only the intermediate nodes in the earliest path can get the rewards according to their contribution time. Then, we can have the following theorem.

Theorem 2: The payment of the source node for each delivered message in the EPSR scheme is upper bounded.

Proof: According to (5), the payment of source node S for a delivered message m_k in the EPSR scheme is

$$\text{Pay}(S,m_k) = \sum_{\forall v_i \in P} Rd(v_i,P) = \sum_{\forall v_i \in P} Ct(v_i,P) = \text{TTL} - t_r \leq \text{TTL}.$$

This suggests that the payment of the source node for each delivered message is upper bounded by the TTL. ■

According to Theorem 2, we can conclude that the EPSR scheme is applicable under the scenario where each node has a finite budget.

Lemma 1: It is deficit free[4] for the TTP in the EPSR scheme.

Proof: Since the source node only needs to pay the rewards to the nodes on the earliest delivery path, it is obvious that the payment is not less than the total rewards for any given transaction. Thus, it is deficit free for the TTP. ■

Lemma 1 can prevent the malicious node from making extra profit from false transactions.

[2] paper, an

[3] If node v_i forwards m_k to more different nodes, it will have a higher probability of being in the earliest path of m_k.

[4] "Deficit free" here means that the payment from the source node for any given transaction is no less than the amount of the total rewarding credits.

3) Security: As the nodes in the network are selfish, they may cheat the system to get extra rewards by conducting malicious behaviors. To analyze the security of the EPSR scheme, we assume that node v_i holds a message m_k while meeting with node v_j. We will discuss if v_i will conduct the malicious behaviors when it forwards m_k to v_j.

Theorem 3: In the EPSR scheme, node v_i has no incentive to launch the edge insertion attack, the edge removal attack, or the content modification attack.

Proof: Suppose P is the earliest delivery path of m_k. For the case that $v_i \notin P$ and $v_j \notin P$, launching one of the three attacks when it forwards m_k to v_j cannot make any benefit for v_i since $Rd(v_i, m_k)$ is always 0. For the case that $v_i \in P$ and $v_j \notin P$, suppose P' is another delivery path of m_k, where $v_i \in P'$ and $v_j \in P'$. Then, v_i has no incentive to launch one of the three attacks, which can only modify $Ct(v_i, P')$, indicating that $Rd(v_i, m_k)$ will not be changed. For the case that $v_i \in P$ and $v_j \in P$, we will consider the three attacks, respectively.

1) Edge insertion attack: As $v_i \in P$, $Rd(v_i, m_k) = Ct(v_i, P)$. Without loss of generality, if node v_i inserts an edge $\overrightarrow{v_i v_{i+1}}$ (v_{i+1} is the sybil of v_i) to P, then both v_i and v_{i+1} will get rewards from the TTP. However, $Ct'(v_i, P) + Ct'(v_{i+1}, P) = Ct(v_i, P)$, where $Ct'(\cdot)$ indicates the contribution time after inserting the edge. Thus, v_i cannot make extra profit by inserting an edge, indicating that it has no incentive to launch an edge insertion attack.
2) Edge removal attack: If v_i launches an edge removal attack, i.e., v_i removes one of the elements from the contribution table, it will break the encryption chain. Then, the contribution table cannot be totally decrypted after being submitted to the TTP, and there will be no reward paid to the nodes. Thus, launching an edge removal attack will make $Rd(v_i, m_k)$ become 0. Therefore, v_i has no incentive to launch an edge removal attack.
3) Content modification attack: As $Rd(v_i, m_k) = Ct(v_i, P)$, v_i may modify the content of its contribution element, such as decreasing t_i^r or increasing t_i^t, to increase $Ct(v_i, P)$. However, such modifications can be detected. Suppose the parent node of v_i is v_k, then in the contribution table, it must satisfy $t_i^r = t_k^t$ and $t_i^t = t_j^r$. Moreover, v_i cannot modify t_k^t or t_j^r since it does not have the private keys of v_k and v_j. Thus, the modification of t_i^r and t_i^t can be easily detected, making v_i get no reward. Consequently, v_i has no incentive to launch a content modification attack.

【思考】dest
如果修改了
report message
里面的path
就可以少付
credit.

中继节点没有理由 发起~

Thus, the EPSR scheme can prevent the nodes from launching the edge insertion attack, the edge removal attack, the content modification attack, or the combination of them. ∎

V. Earliest Path Cumulative Rewarding Scheme

In the EPSR scheme, we have proved that it is incentive compatible for each node to truthfully forward the messages. However, if a node is aware of more contact information of other nodes, it may not work. For example, in Fig. 2, there are three source-to-destination paths. Node A receives message m_k from S at 10:15 A.M., and then, it meets B at 10:35 A.M.

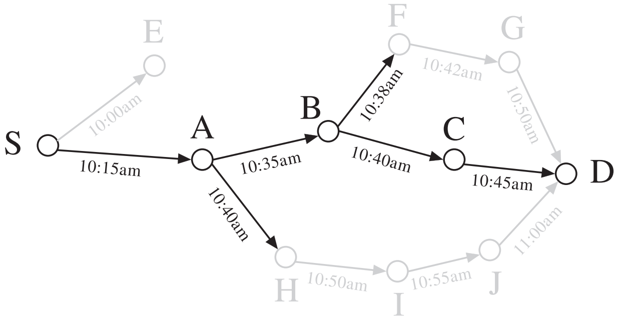

Fig. 4. Total contribution time to be rewarded for the example in Fig. 2 under the EPCR scheme. The gray parts will [illegible] rewarded contribution time.

如果节点A知道 还有另外一个path.
节点A 促使消息能在手里 停留更长的时
间，以获得更多的奖励

If A does not know the contact information of others, it will truthfully forward m_k to B to increase its probability to be in the earliest delivery path. Thus, $Rd(A, m_k) = 20$. However, if A knows that there are only three source-to-destination paths and each of them includes A, i.e., node A becomes a "bridge node" from the source to the destination, then it may not choose to forward m_k to B at 10:35 A.M. Instead, it can forward m_k to H at 10:40 A.M. This way, $Rd(A, m_k) = 25$, which is more than 20. Thus, the EPSR scheme may be not applicable under such scenario. To solve this problem, we will propose the EPCR scheme in this section.

A. EPCR Scheme

The main idea of the EPCR scheme is to reward each node in the earliest delivery path in a cumulative way. To motivate each node to forward the message for every contact, the TTP will reward each node for its efforts on all the delivery paths (including the earliest delivery path and other delivery paths) of each message. Therefore, the reward to each node includes two parts: its contribution time in the earliest delivery path and that in other delivery paths. The latter part of the reward will contribute to motivating the node to truthfully forward the message to its encounter during every contact, even if it is aware of the contact information of others. For example, if the node knows that it is the "bridge node" from the source to the destination, it will also have incentive to forward message each time it meets any other node. All the reward will be paid by the source node. Similar to EPSR, the EPCR scheme includes four phases: system initialization, message generation, message forwarding, and rewarding and charging. The main difference between EPCR and EPSR is in the last phase.

分叉节点

Before introducing the details of the EPCR scheme, we first introduce the concept of *furcation node* of two paths: A furcation node of two paths is the last intersection node (except the destination node) of the two paths. The furcation node of paths P_j and P_k, which is denoted as $Fn(P_j, P_k)$, is mathematically defined as follows.

Definition 1: $Fn(P_j, P_k) : \exists e_l, e_m$ such that $v_i \in e_l$, $e_l \in P_j$, $e_l \notin P_k$ and $v_i \in e_m$, $e_m \in P_k$, $e_m \notin P_j$; then, $Fn(P_j, P_k) = v_i$.

For example, in Fig. 4, node A is the furcation node of path $S \to A \to B \to C \to D$ and path $S \to A \to H \to I \to J \to D$ since it is the last intersection node except node D of the two paths. Similarly, node B is the furcation node of path $S \to A \to B \to C \to D$ and path $S \to A \to B \to F \to G \to D$. Note that according to Definition 1, $Fn(P_j, P_k) = \emptyset$ if $j = k$, i.e., if two paths are the same, they will have no furcation node.

In the rewarding and charging phase, only the nodes in the earliest delivery path can get the rewards. However, the reward to each node is different with that of the EPSR scheme. Suppose the set of all the delivery paths of message m_k is $\mathbb{P}^k = \{P_1, P_2, \ldots, P_l\}$ and P is the earliest delivery path of m_k, i.e., $P = \arg\min\{t(P_i) | \forall P_i \in \mathbb{P}^k\}$. Then, the reward to each node v_i in P for the delivery of m_k is

$$Rd(v_i, m_k) = Ct(v_i, P) + \sum_{j=1}^{l} [w(v_i, P_j) \cdot Ct(v_i, P_j)] \quad (6)$$

where

$$w(v_i, P_j) = \begin{cases} 1, & \text{if } v_i{=}Fn(P,P_j), \forall\, m \in [1,j), v_i \neq Fn(P,P_m) \\ 0, & \text{elsewhere.} \end{cases}$$

给分叉点更多的奖励

Similar to the EPSR scheme, the reward for the delivery of m_k will be paid by the source node, which is denoted as $\text{Pay}(S, m_k)$, where

$$\text{Pay}(S, m_k) = \sum_{\forall v_i \in P} Rd(v_i, P). \quad (7)$$

怎么做到的？
在dest收到两个path来的消息？

Take Fig. 2 for example, after the delivery of m_k, nodes A, B, and C will get rewards from the TTP. As shown in Fig. 4, according to (6), $Rd(A, m_k) = (10{:}35\ \text{A.M.} - 10{:}15\ \text{A.M.}) + (10{:}40\ \text{A.M.} - 10{:}15\ \text{A.M.}) = 45$, $Rd(B, m_k) = (10{:}40\ \text{A.M.} - 10{:}35\ \text{A.M.}) + (10{:}38\ \text{A.M.} - 10{:}35\ \text{A.M.}) = 8$, and $Rd(C, m_k) = (10{:}45\ \text{A.M.} - 10{:}40\ \text{A.M.}) = 5$. The EPCR scheme can solve the problem in the previous scenario as follows: If A does not forward m_k to B at 10:35 A.M. and waits until 10:40 A.M. to forward m_k to H, then the path $S \to A \to H \to I \to J \to D$ will be the earliest delivery path and $Rd(A, m_k) = 25$. However, if A truthfully forwards m_k to each of its encounters, then $Rd(A, m_k) = 45$. Thus, A will truthfully forward the message during every contact opportunity.

B. Analysis

1) Incentive Compatibility: In the initialization phase of the EPCR scheme, the system will provide each node with a small amount of credits, which can only afford the cost for delivering several messages. Thus, each node will act in a risk-averse way to maximize its probability to get the reward.

Theorem 4: The EPCR scheme is incentive compatible.

Proof: As each node will act in a risk-averse way, it will always adopt a strategy to maximize its probability to get the reward. Suppose node v_i holds a message m_k, when it meets v_j, it has two candidate strategies, i.e., v_i forwards m_k to v_j or not. If v_i forwards m_k to v_j, its probability to be in the earliest path of m_k will increase, indicating a higher probability to get the reward. Moreover, the forwarding of m_k to v_j may increase $Rd(v_i, m_k)$ since it may make v_i be the furcation node between the earliest delivery path and another path. However, if v_i does not forward m_k to v_j, its probability to be in the earliest path of m_k will decrease, indicating a lower probability to get the reward. As a risk-averse node, v_i will decide to truthfully forward m_k to v_j. Thus, the EPCR scheme is incentive compatible. ■

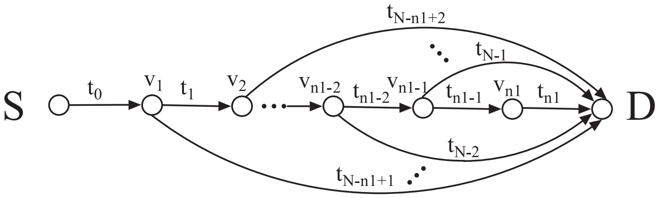

Fig. 5. Case for the maximum payment of the EPCR. The time on each arrow denotes the transmitting time and $t_j - t_i = (j - i) \cdot T$, where $j > i$.

Theorem 4 can guarantee that each node will truthfully forward the messages during every contact opportunity.

2) Budget Issue: In DTNs, the transmission of a message requires some time period due to the limited transmission bit rate. We denote the time to transmit a unified-size message as T. Thus, the upper bound of the number of nodes in a delivery path is $N = \lfloor \text{TTL}/T \rfloor$ (we only consider the number of the transmitters, i.e., N does not include the destination).

Theorem 5: The maximum payment of the source node for a delivered message m_k in the EPCR scheme is

$$\max\ \text{Pay}(S, m_k) = \begin{cases} f\left(\min\left\{\frac{N+1}{2}, n-2\right\}\right) \cdot T, & \text{if N is odd} \\ f\left(\min\left\{\frac{N}{2}+1, n-2\right\}\right) \cdot T, & \text{elsewhere} \end{cases}$$

where $f(x) = -x^2 + (N+3)x - N - 1$, $N = \lfloor \text{TTL}/T \rfloor$, n is the number of nodes in the network, and T is the time to transmit a unified-size message.

Proof: Suppose that message m_k is generated by source node S at t_0 and S immediately transmits m_k to node v_1. After that, m_k is forwarded along nodes $v_1, v_2, \ldots, v_{n_1}$ and then to destination node D, and the path $S \to v_1 \to v_2 \to \cdots \to v_{n_1} \to D$ is the earliest delivery path. Then, a case for S to pay the maximum credits is shown in Fig. 5, that is, v_{n_1-1} will transmit m_k directly to D at time t_{N-1}, and v_{n_1-2} will transmit m_k directly to D at time t_{N-2}, and so on.

According to (6), after the delivery of m_k, v_1 can get a reward of $(t_1 - t_0) + (t_{N-n_1+1} - t_0)$. Note that the last intermediate node v_{n_1} can only get a reward of $(t_{n_1} - t_{n_1-1})$ as it only has such amount of contribution time in the earliest path. According to (7), the payment of S is

$$\begin{aligned} \text{Pay}(S, m_k) &= [(t_1 - t_0) + (t_{N-n_1+1} - t_0)] \\ &\quad + [(t_2 - t_1) + (t_{N-n_1+2} - t_1)] \\ &\qquad + \cdots + [(t_{n_1-1} - t_{n_1-2}) + (t_{N-2} - t_{n_1-1})] \\ &\qquad + (t_{n_1} - t_{n_1-1}) \\ &= (t_{n_1} - t_0) + \sum_{i=1}^{n_1-1} (t_{N-n_1+i} - t_{i-1}) \\ &= n_1 \cdot T + (n_1 - 1)(N - n_1 + 1) \cdot T \\ &= \left[-n_1^2 + (N+3)n_1 - N - 1\right] \cdot T. \end{aligned}$$

It is obvious that $\text{Pay}(S, m_k)$ is an increasing function of n_1 when $n_1 < (N+3)/2$.

As the path $S \to v_1 \to v_2 \to \cdots \to v_{n_1} \to D$ is the earliest delivery path of m_k, the moment that node v_{n_1} transmits m_k to D is at least T earlier than other moments that m_k is transmitted to D by other nodes. Thus, $t_{n_1} \leq t_{N-n_1+1} + T$, i.e., $n_1 \leq N - n_1 + 2$. Hence, n_1 must satisfy $n_1 \leq N/2 + 1$. Moreover, as the number of all the nodes is n, we can get $n_1 + 2 \leq n$ (n_1 is the number of nodes in the earliest path except the source and the destination).

Thus, we can get

$$\text{Pay}(S, m_k) = \left[-n_1^2 + (N+3)n_1 - N - 1\right] \cdot T$$

where $n_1 \leq N/2 + 1$ and $n_1 \leq n - 2$.

Hence, if N is an odd number, $\text{Pay}(S, m_k)$ will be the largest when $n_1 = \min\{(N-1)/2 + 1,\ n-2\}$. Otherwise, if N is an even number, $\text{Pay}(S, m_k)$ will be the largest when $n_1 = \min\{N/2 + 1,\ n-2\}$. Thus

$$\max\ \text{Pay}(S, m_k) = \begin{cases} f\left(\min\left\{\frac{N+1}{2}, n-2\right\}\right) \cdot T, & \text{if N is odd} \\ f\left(\min\left\{\frac{N}{2}+1, n-2\right\}\right) \cdot T, & \text{elsewhere.} \end{cases} \quad (8)$$

■

Lemma 2: The payment of the source node for each delivered message in the EPCR scheme is upper bounded.

Proof: The maximum payment of the source node for a delivered message m_k in the EPCR scheme is formulated in (8). Since the function $f(\cdot)$ in (8) is continuous and all the parameters N, TTL, and n are finite, it is obvious that the payment of the source node for each delivered message in the EPCR scheme is upper bounded. ■

According to Lemma 2, we can conclude that the EPCR scheme is applicable under the scenario that each node has a finite budget. Although the bound of the payment of the source node for each delivered message may seem large, we argue that it is feasible in practice since the reward to each node for the delivered message also increases.

Lemma 3: It is deficit free for the TTP in the EPCR scheme.

Proof: Since the payment of the source node for each delivered message is equal to the total rewards paid to the nodes in the earliest delivery path of the message, the EPCR scheme is budget balance. Thus, it is deficit free for the TTP. ■

Lemma 3 guarantees the property of being deficit free of the EPCR scheme, which can prevent the malicious node from making profit by phantom transactions.

3) Security: Due to natural selfishness, each node may launch one of the three attacks to get more reward. Here, we will discuss the security issue of the EPCR scheme. Similarly, we assume that node v_i holds a message m_k while meeting v_j. Then, we discuss if v_i will conduct the attacks when it forwards m_k to v_j.

Theorem 6: In the EPCR scheme, node v_i has no incentive to launch the edge insertion attack, the edge removal attack, or the content modification attack.

Proof: Suppose P is the earliest delivery path of m_k. For the case that $v_i \notin P$ and $v_j \notin P$, v_i has no incentive to launch one of the three attacks before forwarding m_k to v_j as $Rd(v_i, m_k)$ is still 0. For the other cases that $v_i \in P$ and $v_j \in P$, or $v_i \in P$ and $v_j \notin P$, we will consider the three attacks, respectively.

1) Edge insertion attack: If ~~$v_i \in P$ and $v_j \notin P$,~~ then v_i can get the reward according to (6). For instance, suppose $v_j \in P'$, where P' is not the earliest path, then if v_i inserts an edge between itself and v_j such as $\overrightarrow{v_i v_{i+1}}$, then P' will contain $\overrightarrow{v_i v_{i+1}}$ and $\overrightarrow{v_{i+1} v_j}$, and $Rd(v_{i+1}, m_k) = 0$ since $v_{i+1} \notin P$. Consequently, $Ct(v_i, P')$ will be reduced by $t_{i+1}^t - t_{i+1}^r$ as the time interval between v_i and v_j in path P' cannot be modified, where t_{i+1}^r is the time that v_{i+1} receives m_k from v_i, and t_{i+1}^t is the time that v_{i+1} transmits m_k to v_j. Note that t_{i+1}^r and t_{i+1}^t are determined by v_i, and they must satisfy $t_i^r < t_{i+1}^r < t_j^r$ and $t_{i+1}^t = t_j^r$. Thus, launching an edge insertion attack will reduce $Rd(v_i, m_k)$ (since v_i is the furcation node between P and P', thus $Ct(v_i, P')$ will be included in $Rd(v_i, m_k)$), leading to loss of incentive to do that. On the other case that $v_i \in P$ and $v_j \in P$, if v_i inserts an edge between itself and v_j, similarly assume v_i inserts a sybil node v_{i+1} between itself and v_j, then $Ct'(v_i, P) + Ct'(v_{i+1}, P) = Ct(v_i, P)$, where $Ct'(\cdot)$ denotes the contribution time after inserting the edge. Then, v_i cannot increase $Rd(v_i, P)$ after inserting the edge. Thus, v_i has no incentive to launch an edge insertion attack.

For the proof of defense against the edge removal attack and the content modification attack of the EPCR scheme, as it is similar to that of the EPSR scheme shown in Theorem 3, we omit the proof here to save space. ■

According to Theorem 6, the EPCR scheme can prevent the nodes from launching the edge insertion attack, the edge removal attack, the content modification attack, or the combination thereof.

VI. Performance Evaluation

Here, we evaluate the proposed rewarding schemes in the Opportunistic Network Environment simulator [28] using the UMassDieselNet trace [19], which was collected based on a real bus-based DTN testbed composed of 30 buses operated by the UMass Amherst branch of the Pioneer Valley Transport Authority. The used UMassDieselNet trace was the contact information recorded by the nodes deployed on the 30 buses for 60 days. Our objectives are threefold: 1) to illustrate the necessity of the rewarding schemes to motivate the cooperation in the message forwarding; 2) to validate the feasibility of the proposed rewarding schemes; and 3) to analyze the effects of the network parameters on the proposed rewarding schemes.

A. Simulation Setup

We set the parameters in the simulations as follows: The size of each message is 1 KB, and the buffer space of each node is 1 GB; thus, the effects of insufficient buffer space on the performance will be excluded in the simulations. The transmission rate is 2 Mb/s. The default number of generated messages during the whole period of simulation is 1500, and the default TTL of each message is 3000 min. In the simulations, one unit of the rewarding credit corresponds to 1 s of the contribution time.

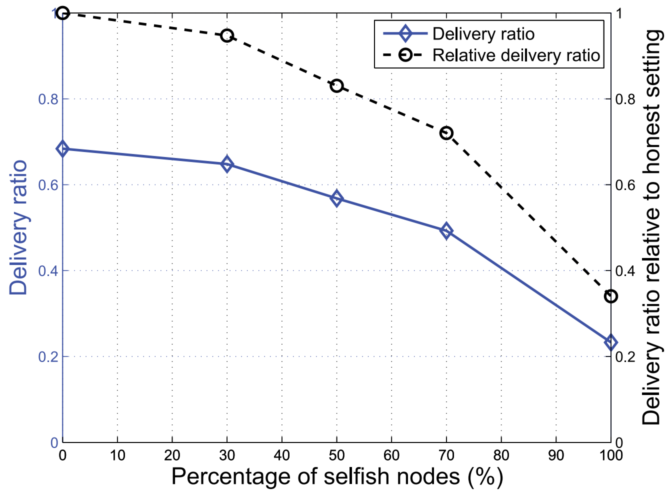

Fig. 6. Delivery ratio and relative delivery ratio under different percentage values of selfish nodes.

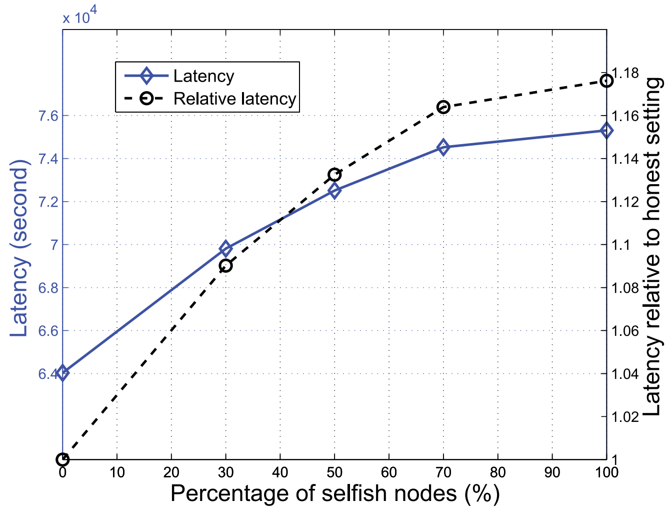

Fig. 7. Latency and relative latency under different percentage values of selfish nodes.

B. Simulation Results

In Figs. 6 and 7, the impacts of selfish nodes on the DTN routing performance are analyzed under the scenario that no rewarding scheme is adopted, in which some percentage of nodes will behave selfishly. In the simulations, a selfish node will act in a free-riding way such that it will only forward its own generated messages but refuse to forward those generated by other nodes. In these two figures, the number of generated messages is set as 1500, and the TTL of each message is set as 3000 min. Fig. 6 shows the effects of the selfish nodes on the delivery ratio and the relative delivery ratio. The solid-line curve in Fig. 6 shows the decrease trend of the delivery ratio when the percentage of selfish nodes increases. When all the nodes are nonselfish, i.e., the percentage of selfish nodes is equal to 0, then the delivery ratio can be almost 70%, which is high enough for many practical applications. When all the nodes are selfish, i.e., the percentage of selfish nodes is equal to 100%, the delivery ratio drops dramatically to only 22%. Note that the delivery ratio with 100% selfish nodes can be larger than 0 since each source node may have a chance to directly deliver its own generated message to the destination. The dashed curve in Fig. 6 shows the decrease trend of the delivery ratio relative to that with no selfish node. It clearly shows the downgrade percentage of the delivery ratio when more selfish nodes exist.

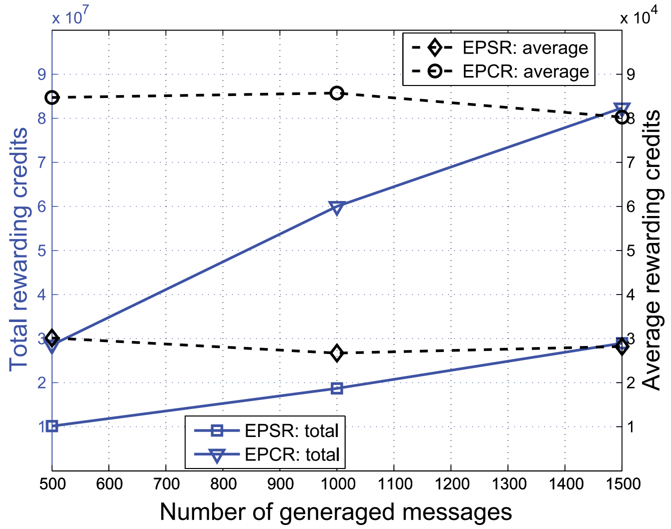

Fig. 8. Total rewarding credits and average rewarding credits of the two proposed rewarding schemes under different numbers of generated messages.

Fig. 7 shows the effects of the selfish nodes on latency and relative latency. The solid-line curve reflects the increase trend of the latency when the percentage of selfish nodes increases. It shows that the latency is only 64 000 s when all the nodes are nonselfish. When the percentage of selfish nodes increases, the latency will rise dramatically. The latency will reach 75 300 s under the extreme case that all the nodes are selfish. The dashed curve clearly shows the increase percentage of the latency with different percentage values of selfish nodes. It is illustrated that the latency will increase to 118% of that with no selfish nodes. As shown in Figs. 6 and 7, the existence of the selfish nodes will dramatically decrease the delivery ratio and increase the latency. Thus, the effects of the selfish nodes on the message forwarding cannot be ignored, and it is highly necessary to propose the rewarding schemes to motivate cooperation in the message forwarding.

As previously mentioned, the proposed rewarding schemes are incentive compatible, i.e., all the nodes in the network will truthfully forward the messages. Figs. 8 and 9 show the effects of the network parameters on the proposed two rewarding schemes. Fig. 8 shows the total rewarding credits and average rewarding credits of the proposed two rewarding schemes under different numbers of generated messages (from 500 to 1500), respectively. Here, the total rewarding credits mean the summation of the rewarding credits of all the delivered messages in the network, and the average rewarding credits mean the average rewarding credits for each delivered message, i.e., the average rewarding credits is equal to the total rewarding credits over the number of delivered messages. The TTL of each message in Fig. 8 is set as 3000 min. The solid-line curves depict the total rewarding credits of the two rewarding schemes, which increase

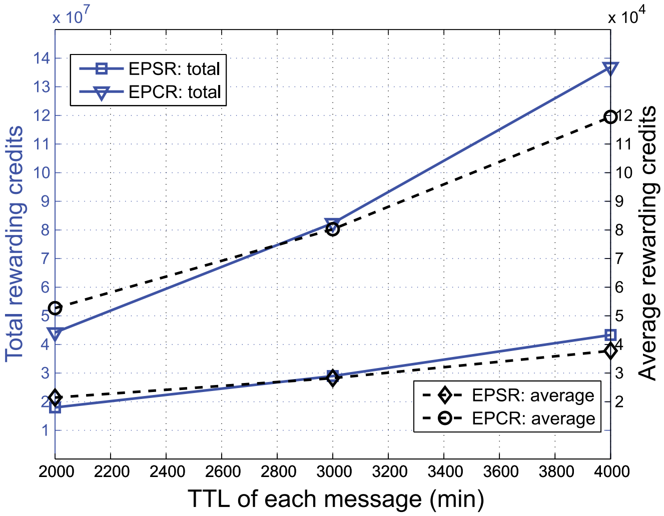

Fig. 9. Total rewarding credits and average rewarding credits of the two proposed rewarding schemes under different TTL of each message.

almost linearly with the number of generated messages. Since the increase in the number of generated messages will increase the number of delivered messages, the total rewarding credits will increase linearly with the number of generated messages. As the EPCR scheme rewards each node in the earliest delivery path in a cumulative manner, the total rewarding credits are more than that of the EPSR scheme. The dashed curves depict the average rewarding credits for each delivered message of the two rewarding schemes, respectively. Similarly, the average rewarding credits of the EPCR scheme are more than that of the EPSR scheme. It shows hat the average rewarding credits of the two proposed rewarding schemes are quite stable under different numbers of generated messages, which validates our previous claim that the payment of the source node for each delivered message is upper bounded (as the rewarding credits are charged from the source node).

Fig. 9 shows the effects of the TTL of each message, which varies from 2000 to 4000 min with the interval of 1000 min, on the total rewarding credits and average rewarding credits of the proposed two rewarding schemes, respectively. The meaning of the total rewarding credits and average rewarding credits is the same as that in Fig. 8. The solid-line curves illustrate the effects of the TTL on the total rewarding credits of the two rewarding schemes. The increase of the TTL will increase the total rewarding credits of the two rewarding schemes. As the rewarding credits of the two schemes are based on the contribution time of the nodes, the increase of the TTL may increase the total contribution time of the nodes in each delivery path, and the number of delivered messages will also increase with the increase of TTL, which will result in more total rewarding credits. Fig. 9 shows that the total rewarding credits of the EPCR scheme are more than that of the EPSR scheme. The dashed curves illustrate the effect of the TTL on the average rewarding credits for each delivered message, which shows that the average credits of the two rewarding schemes increase almost linearly with the TTL. Similarly, the average rewarding credits of the EPCR scheme are more than that of the EPSR scheme.

VII. Conclusion

In this paper, by considering the drawbacks of the previous incentive schemes, we have proposed the EPSR and EPCR schemes, respectively, to motivate the nodes to cooperate with each other in the message forwarding. We prove that the proposed rewarding schemes are incentive compatible, which guarantees that the dominant strategy for the nodes is to truthfully forward the messages. It is also proved that the payment for each delivered message is upper bounded, making the proposed rewarding schemes applicable for the scenario when the nodes have a finite budget. Furthermore, the proposed rewarding scheme is resistant to the malicious behaviors of the selfish nodes. We conduct the simulations based on the real trace to illustrate the effectiveness of the proposed rewarding schemes.

References

[1] H. Chen and W. Lou, “On using contact expectation for routing in delay tolerant networks,” in *Proc. IEEE ICPP*, 2011, pp. 683–692.

[2] S. He *et al.*, “EMD: Energy-efficient delay-tolerant P2P message dissemination in wireless sensor and actor networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 75–84, Sep. 2013.

[3] J. A. F. F. Dias, J. J. P. C. Rodrigues, C. Mavromoustakis, and F. Xia, “A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks,” *IEEE Trans. Ind. Electron.*, DOI: 10.1109/TIE.2015.2425357, vol. 62, no. 12, pp. 7929–7937, Dec. 2015.

[4] J. Molina-Gil and P. C.-G. C. Caballero-Gil, “Aggregation and probabilistic verification for data authentication in VANETs,” *Elsevier Inf. Sci.*, vol. 262, pp. 172–189, Mar. 2014.

[5] P. R. Pereira, A. Casaca, J. J. P. C. Rodrigues, and V. N. G. J. Soares, “From delay-tolerant networks to vehicular delay-tolerant networks,” *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 1166–1182, 4th Quart. 2012.

[6] T. Chen, L. Zhu, F. Wu, and S. Zhong, “Stimulating cooperation in vehicular ad hoc networks: A coalitional game theoretical approach,” *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 566–579, Feb. 2011.

[7] J. Wu, M. Xiao, and L. Huang, “Homing spread: Community home-based multi-copy routing in mobile social networks,” in *Proc. IEEE INFOCOM*, 2013, pp. 2319–2327.

[8] Z. Wang, J. Liao, Q. Cao, H. Qi, and Z. Wang, “Friendbook: A semantic-based friend recommendation system for social networks,” *IEEE Trans. Mobile Comput.*, vol. 14, no. 3, pp. 538–551, Mar. 2015.

[9] A. Chaintreau *et al.*, “Impact of human mobility on the design of opportunistic forwarding algorithms,” in *Proc. IEEE INFOCOM*, 2007, pp. 606–620.

[10] A. Vahdat and D. Becker, “Epidemic routing for partially-connected Ad Hoc networks,” Duke Univ., Durham, NC, USA, Tech. Rep. CS-200006, Apr. 2000.

[11] F. Li, J. Wu, and A. Srinivasan, “Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets,” in *Proc. IEEE INFOCOM*, 2009, pp. 2428–2436.

[12] B. B. Chen and M. C. Chan, “MobiCent: A credit-based incentive system for disruption tolerant network,” in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[13] U. Shevade, H. H. Song, L. Qiu, and Y. Zhang, “Incentive-aware Routing in DTNs,” in *Proc. IEEE ICNP*, 2008, pp. 238–247.

[14] S. Zhong, L. Li, Y. G. Liu, and Y. R. Yang, “On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks—An integrated approach using game theoretical and cryptographic techniques,” in *Proc. ACM MobiCom*, 2005, pp. 799–816.

[15] H. Zhou, J. Chen, J. Fan, Y. Du, and S. K. Das, “ConSub: Incentive-based content subscribing in selfish opportunistic mobile networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 669–679, Sep. 2013.

[16] X. Y. Li, Y. Wu, P. Xu, G. Chen, and M. Li, “Hidden information and actions in multi-hop wireless ad hoc networks,” in *Proc. ACM MobiHoc*, 2008, pp. 1–10.

[17] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, “SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks,” *IEEE Trans. Veh. Technol.*, vol. 58, no. 8, pp. 4628–4639, Oct. 2009.

[18] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," in *Proc. ACM MobiHoc*, 2003, pp. 1–8.

[19] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "MaxProp: Routing for vehicle-based disruption-tolerant networking," in *Proc. IEEE INFOCOM*, 2006, pp. 1–11.

[20] V. Erramilli, M. Crovella, A. Chaintreau, and C. Diot, "Delegation forwarding," in *Proc. ACM MobiHoc*, 2008, pp. 251–259.

[21] Q. He, D. Wu, and P. Khosla, "SORI: A secure and objective reputation based incentive scheme for ad hoc networks," in *Proc. IEEE WCNC*, 2004, pp. 825–830.

[22] M. Y. S. Uddin, B. Godfrey, and T. Abdelzaher, "RELICS: In-network realization of incentives to combat selfishness in DTNs," in *Proc. IEEE ICNP*, 2010, pp. 203–212.

[23] X. Zhang, G. Xue, R. Yu, D. Yang, and J. Tang, "Truthful incentive mechanisms for crowdsourcing," in *Proc. IEEE INFOCOM*, 2015, pp. 2830–2838.

[24] S. Buchegger and J. L. Boudec, "Performance analysis of the CONFIDANT protocol (Cooperation of nodes: Fairness in dynamic ad-hoc networks)," in *Proc. ACM MobiHoc*, 2002, pp. 226–236.

[25] K. Srinivasan, S. Rajkumar, and P. Ramanathan, "Incentive schemes for data collaboration in disruption tolerant networks," in *Proc. IEEE GLOBECOM*, 2010, pp. 1–5.

[26] A. Krifa, C. Barakat, and T. Spyropoulos, "Mobitrade: Trading content in disruption tolerant networks," in *Proc. ACM CHANTS*, 2011, pp. 31–36.

[27] I. N. Kovalenko and A. I. Kochubinskii, "Asymmetric cryptographic algorithms," *Cybern. Syst. Anal.*, vol. 39, no. 4, pp. 549–554.

[28] A. Keranen, J. Ott, and T. Karkkainen, "The ONE simulator for DTN protocol evaluation," in *Proc. 2nd Int. Conf. SIMUTools*, 2009, p. 22.

[29] H. Chen and W. Lou, "Making nodes cooperative: A secure incentive mechanism for message forwarding in DTNs," in *Proc. IEEE ICCCN*, 2013, pp. 1–7.

Honglong Chen (M'15) received the B.E. degree in automation from China University of Petroleum, Beijing, China, in 2006; the M.E. degree from the Department of Control, Zhejiang University, Hangzhou, China, in 2008; and the Ph.D. degree in computer science from The Hong Kong Polytechnic University, Kowloon, Hong Kong, in 2012.

He is currently an Associate Professor with the College of Information and Control Engineering, China University of Petroleum. His research interests include wireless sensor networks, delay-tolerant networks, and mobile ad hoc networks. His research is supported by the National Natural Science Foundation of China Grant and the Shandong Provincial National Science Foundation Grant.

Dr. Chen is a member of the Association for Computing Machinery.

Wei Lou (M'14) received the B.E. degree in electrical engineering from Tsinghua University, Beijing, China, in 1995; the M.E. degree in telecommunications from Beijing University of Posts and Telecommunications, in 1998; and the Ph.D. degree in computer engineering from Florida Atlantic University, Boca Raton, FL, USA, in 2004.

He is currently an Assistant Professor with the Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong. His current research interests include wireless networking, mobile ad hoc and sensor networks, peer-to-peer networks, and mobile cloud computing. He has worked intensively on designing, analyzing, and evaluating practical algorithms with the theoretical basis, as well as building prototype systems. His research work is supported by several Hong Kong General Research Fund Grants and Hong Kong Polytechnic University Interdisciplinary/Collaborative Research Grants.

Zhibo Wang (M'15) received the B.E. degree in automation from Zhejiang University, Hangzhou, China, in 2007 and the Ph.D. degree in electrical engineering and computer science from The University of Tennessee, Knoxville, TN, USA, in 2014.

He is currently an Associate Professor with the School of Computer, Wuhan University, Wuhan, China. His current research interests include wireless sensor networks, cyberphysical systems, and mobile sensing.

Dr. Wang is a member of the Association for Computing Machinery.

Qian Wang (M'14) received the B.S. degree from Wuhan University, Wuhan, China, in 2003; the M.S. degree from the Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, China, in 2006; and the Ph.D. degree from Illinois Institute of Technology, Chicago, IL, USA, in 2012, all in electrical engineering.

He is currently a Professor with the School of Computer Science, Wuhan University. His research interests include wireless network security and privacy, cloud computing security, and applied cryptography.

Dr. Wang is an expert under the "1000 Young Talents Program" of China. He coreceived the Best Paper Award from the 2011 IEEE International Conference on Network Protocols. He is a member of the Association for Computing Machinery.